UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

VAN GROSS, on behalf of himself and all others similarly situated, Plaintiff, v. HEALTHEC, LLC, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Van Gross, ("Gross" or "Plaintiff"), by and through his attorneys of record, upon personal knowledge as to his own acts and experiences, upon investigation of counsel, and upon information and belief as to all other matters, brings this class action complaint against defendant HealthEC, LLC ("HealthEC" or "Defendant"), and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action on behalf of a Class, as defined below, against Defendant for its failure to properly secure and safeguard Plaintiff's and Class Members' protected personal health information stored within Defendant's information networks and servers, including, without limitation, "protected health information" ("PHI"),[1] and "personally

[1] Protected Health Information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories, and data points applied to a set of demographic information for a particular patient. PHI is inclusive of and incorporates personally identifiable information.

identifiable information" ("PII"),[2] as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, PHI and PII are also referred to therein as "Private Information").

2. Defendant HealthEC, headquartered in Edison, New Jersey, provides technology services to healthcare organizations and provides services such as data integration, analytics, care coordination, patient engagement, compliance, and reporting.

3. Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and other similarly situated persons by virtue of a massive and preventable cyberattack that occurred between July 14, 2023 and July 23, 2023, by which cybercriminals infiltrated Defendant's electronic data storage networks and systems, in or on which the Private Information of Plaintiff and Members of the Class was stored (the "Data Breach"). Defendant collected, stored, and maintained the Private Information of Plaintiff and the Class and Defendant was responsible for securing said Private Information. Plaintiff further seeks to hold Defendant responsible for not ensuring that PII and PHI, as defined by HIPAA Privacy Rule (45 CFR, Parts 160 and 164(A) and (E)), and respecting which it was duty bound to protect pursuant to the HIPAA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), was maintained in a manner consistent with industry standards, and other relevant standards.

4. HIPAA, in general, applies to healthcare providers, health plans/insurers, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and to and HIPAA business associates that create, receive, maintain, or transmit PHI, and sets standards for Defendant's maintenance of Plaintiff's and Class Members' PII and PHI, including appropriate safeguards to be maintained by organizations such as Defendant's to

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

protect the privacy of patient health information, while setting limits and conditions on the uses and disclosures that may be made of such information without express customer/patient authorization.

5. Additionally, the so-called "HIPAA Security Rule" establishes national standards to protect individuals' electronic health information that is created, received, used, or maintained by a covered entity such as Defendant. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI. HIPAA provides the standard of procedure by which a medical provider must operate when collecting, storing, and maintaining the confidentiality of PHI and PII information.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' PII and PHI, Defendant knowingly assumed legal and equitable duties to those individuals, including those arising from common law principles.

7. Nonetheless, Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take, implement, and ensure adequate and reasonable measures regarding the safeguarding of Plaintiff's and Class Members' PII and PHI, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data. As a result and upon information and belief, the PII and PHI of Plaintiff and Class Members has been compromised and they have been and shall be damaged through access by and disclosure to an unknown and unauthorized entity—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future. In addition, Plaintiff and Class Members, who have a continuing interest in ensuring that their information is safe, are entitled to injunctive and other equitable relief.

PARTIES

Plaintiff

8. Plaintiff Van Gross is, and at all relevant times was, a resident of Macomb County, Michigan. Plaintiff was and is a patient of Corewell Health, a health care provider that contracts with Defendant. Since receiving notice of the data breach, Plaintiff has been forced to spend time monitoring personal financial accounts for signs of fraudulent transactions or activity. Plaintiff has also noticed a substantial increase in spam phone calls since the Data Breach.

Defendant

9. Defendant HealthEC, LLC is a limited liability company organized under the laws of the State of Delaware, with its principal place of business located at 343 Thornall Street, Suite 630, New Jersey 08837.

JURISDICTION AND VENUE

10. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

11. The District of New Jersey has personal jurisdiction over Defendant because Defendant is a corporation of New Jersey with a principal place of business in this District.

12. This Court is the proper venue for this action because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District, and because Defendant conducts a substantial part of its business within this District.

FACTUAL BACKGROUND

13. Defendant HealthEC is a HIPAA Business Associate, providing technology services to healthcare providers, used by over one million healthcare providers across eighteen states. These services include data integration, analytics, care coordination, patient engagement, compliance, and reporting.

14. As a core part of its business, Defendant collects highly sensitive client and patient data, to create comprehensive patient health records. Defendant also collects financial information, such as health billing information, individual medical history, medication information and other health-related data.

15. Defendant's privacy policy (the "Privacy Policy") assures patients that it is committed to protecting the privacy of the Private Information. Defendant implicitly and/or explicitly represented to Plaintiff and Class Members, that their Private Information would be secured.[3]

16. Defendant had duties and obligations through common law, federal regulations, contracts, industry standards, and their representations to Plaintiff and Class Members that Defendant would adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from third party actors.

The Data Breach

17. On December 22, 2023, Defendant announced, via a post on its website, that, at some undisclosed point in time, it "became aware of suspicious activity potentially involving its network[,]" thereafter determining that between July 14, 2023 and July 23, 2023, certain of its

[3] *See* HealthEC, *Privacy Policy*, https://mneconnect.healthec.com/ProdMNeConnectAdmin/Privacy_Policy.aspx (last accessed January 31, 2024).

systems were "accessed by a known actor" and that, as a result, files were exfiltrated from its systems.[4]

18. As part of its announcement, Defendant stated that it concluded its investigation on or around October 24, 2023, and notified its direct clients on October 26, 2023.[5]

19. Despite Defendant's duties and obligations, Defendant failed to maintain sufficient security to protect its systems. This catastrophic failure led to the Data Breach, affecting 4.5 million individuals. In addition to failing to maintain sufficient security, Defendant allowed months to go by before beginning to send notice to Plaintiff and the members of the Class, which hindered their ability to take affirmative steps to protect themselves from identity theft and financial fraud.

20. On or about December 22, 2024, Plaintiff received a notice of the Data Breach from Defendant which, in addition to the statements above, disclosed that "[y]our name and Name (sic), Address, Date of Birth, Social Security Number, Medical Record Number, Medical Information (such as Diagnosis, Diagnosis Code, Mental/Physical Condition, Prescription information, and provider's name), Health insurance information (such as beneficiary number, subscriber number, Medicaid/Medicare identification), and/or Billing and Claims information (such as patient account number, patient identification number, and treatment and cost information) were present in the impacted files." The Notice of Data Breach received by Plaintiff is attached hereto as Exhibit A.

21. This "disclosure," which came more than five months after Defendant discovered the Data Breach, and two months after it completed its investigation, amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

22. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, and

[4] https://www.healthec.com/cyber-incident/ (Last accessed January 31, 2024).

[5] https://www.healthec.com/cyber-incident/ (Last accessed January 31, 2024).

failed to adhere to the standard of care required of healthcare related business and services, ultimately leading to and causing the exposure of Private Information.

23. Upon information and belief, Defendant continues to inadequately secure or maintain Plaintiff's PHI and PII, as well as that of all other Class Members.

24. Beyond acknowledging the Data Breach – albeit inadequately – Defendant's therapeutic steps are inadequate. Defendant has failed to adequately compensate Plaintiff and members of the Class. It has failed to adequately address the multiple years of identity theft and financial fraud that Data Breach victims face. As a consequence of the Data Breach, Plaintiff and Class Members will be forced to pay out-of-pocket for necessary identifying monitoring services for years thereafter.

As a HIPAA Business Associate, Defendant is Obliged to Preserve and Protect PHI and PII

25. Plaintiff and Class Members are current or former patients of healthcare providers that contract with Defendant, a HIPAA Business Associate and whose PHI and PII is, as a result, provided to Defendant.

26. As a consequence of securing or receiving healthcare services, Plaintiff and Class Members were required to provide sensitive and confidential Private Information, including their names and Social Security Numbers, and other sensitive information.

27. The Private Information of Plaintiff and Class Members was provided to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. Plaintiff and Class Members were reliant on Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary healthcare purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members, who value the confidentiality of their Private Information and demand security to

safeguard their Private Information, took reasonable steps to maintain the confidentiality of their PII/PHI.

29. At all times material, Defendant was under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. To that end, Defendant was reposed with a legal duty created by HIPAA, contract, and industry standards, to keep the Private Information of Plaintiff and the Class confidential and to protect it from unauthorized access and disclosure.

30. By obtaining, collecting, using, and storing Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure. And given the highly sensitive nature of the PII and PHI it possessed and the sensitivity of the medical and health services it provides, Defendant had a duty to safeguard, protect, and encrypt Plaintiff's and Class Members' PII and PHI.

31. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform its services as a HIPAA Business Associate.

32. Upon information and belief, Defendant represented that it would protect the Private Information of Plaintiff and all Class Members from unauthorized disclosure, demonstrating an understanding of the importance of securing Private Information.

33. Defendant's failure to adequately safeguard the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

34. Defendant was not permitted to disclose Plaintiff's and Class Members' Private Information for any reason that would apply in this situation.

35. Defendant was obliged by contract, industry standards, common law, and its own promises and representations to keep the Private Information confidential of Plaintiff and the Class and protect it from unauthorized access and disclosure.

36. Plaintiff and Class Members had a reasonable expectation that Defendant would comply with its obligations to keep their Private Information confidential and secure from unauthorized access and disclosure.

37. Defendant failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, consequently enabling and causing the exposure of Private Information of approximately 4.5 million individuals.

38. Because of Defendant's negligence and misconduct in failing to keep the accessed information confidential, the unencrypted Private Information of Plaintiff and Class Members has been expropriated by unauthorized individuals who can now exploit the PHI and PII of Plaintiff and Class Members and use it as they please.

39. Even though Defendant recognized no later than October 24, 2023, that Private Information had been accessed and exfiltrated, it delayed sending written notice directly to members of the Class.

40. Plaintiff and Class Members now face a real, present, and substantially increased risk of fraud and identity theft.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

41. The PII and PHI of consumers, such as Plaintiff and Class Members, is highly valuable and has been commoditized in recent years.

42. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

43. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

44. Plaintiff and Class Members also suffer ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the financial information in possession of Defendant;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

L. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

45. Moreover, Plaintiff and Class Members have an interest in ensuring that Defendant implements reasonable security measures and safeguards to maintain the integrity and confidentiality of the Private Information, including making sure that the storage of data or documents containing Private Information is not accessible by unauthorized persons, that access to such data is sufficiently protected, and that the Private Information remaining in the possession of Defendant is encrypted, fully secure, remains secure, and is not subject to future theft.

46. As a further direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

47. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized access of and disclosure or risk of exfiltration of Plaintiff's and Class Members' Private Information, Plaintiff and Class Members have suffered, and will continue to suffer, actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they have spent or must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed by unauthorized cyber-thieves in the Data Breach.

Defendant Was Well Aware of the Threat of Cyber Theft and Exfiltration in the Healthcare Industry

48. Defendant was aware of the significant repercussions that would result from its failure to do protect Private Information and knew, or should have known, the importance of safeguarding the Private Information entrusted to it and of the foreseeable consequences if its data security was breached.

49. Defendant could have prevented the Data Breach by assuring that the Private Information at issue was properly secured. Defendant's overt negligence in safeguarding Plaintiff's and Class Members' PII and PHI is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as an entity in the healthcare space, Defendant was on notice that companies in the healthcare industry are targets for data breaches.

50. The healthcare industry in particular has experienced a large number of high-profile cyberattacks. Cyberattacks, generally, have become increasingly more common. In 2021, a record 715 healthcare data breaches reported, an increase of approximately 100% since 2017.[6]

51. This trend continued in 2022, with 707 healthcare breaches reported, still near record highs.[7] Additionally, according to the HIPAA Journal, the five largest healthcare data breaches reported in 2022 impacted the healthcare records of approximately 13.3 million people.[8] Thus, Defendant was on further notice regarding the increased risks of inadequate cybersecurity. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in

[6] 2022 Healthcare Data Breach Report, https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last accessed January 31, 2024).

[7] *Id.*

[8] *Id.*

cyberattacks, including ransomware attacks, urging facilities to shore up their cyber defenses.[9] Indeed, HHS's cybersecurity arm has issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[10]

52. In the context of data breaches, healthcare is "by far the most affected industry sector."[11] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[12]

53. A TENABLE study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of the breaches."[13]

54. This is such a breach of cybersecurity where highly detailed PII and PHI records maintained and collected by a healthcare entity were accessed and/or acquired by a cybercriminal.

55. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place and

---

[9] Rebecca Pifer, Tenet says 'cybersecurity incident' disrupted hospital operations, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-sayscybersecurity-incident-disrupted-hospital-operations/622692/ (last accessed January 31, 2024).

[10] *Id*. (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").

[11] *Id*.

[12] *Id*.

[13] *Id*.

assure the security of the data collected by them and entrusted to them by Plaintiff and Class Members.

56. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII and PHI from being compromised, including failing to encrypt.

Defendant's Conduct Fails to Adhere to Industry Standards, HIPAA and HITECH Standards, and Commensurate Duties it Owed to Plaintiff and the Class

57. Defendant embraced a standard of care and commensurate duty defined by HIPAA, state law and common law to safeguard the PHI and PII of Plaintiff and Class Members data.

58. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data under the condition and implied promise and assurance that it would be kept confidential and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

59. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

60. Defendant is a business associate under HIPAA, subject to the standards and implementation specifications of HIPAA. See 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E.

61. Defendant is also a business associate pursuant to the Health Information Technology Act ("HITECH").[14] See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

62. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

63. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

64. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

65. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

66. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

67. HIPAA's Security Rule requires Defendant to do the following:

a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

[14] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

c) Protect Against reasonably anticipated uses or disclosures of such information that are not permitted; and,

d) Ensure compliance by its workforce.

68. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

69. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

70. Plaintiff's and Class Members' Personal and Medical Information, including their PII and PHI, is "protected health information" as defined by 45 CFR § 160.103.

71. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

72. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

73. Plaintiff's and Class Members' personal and medical information, including their PII and PHI, is "unsecured protected health information" as defined by 45 CFR § 164.402.

74. Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

75. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

76. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

77. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

78. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

79. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

80. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

81. This Data Breach constitutes an unauthorized access of PHI, which is not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

82. The Data Breach could have been prevented if Defendant had implemented HIPAA mandated and industry standard policies and procedures for securely disposing of PHI when it was

no longer necessary and/or had honored its obligations to its patients with respect to adequately securing and maintaining the confidentiality of Private Information.

83. It can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiff's and Class Members' PII and PHI.

84. Upon information and belief, prior to the Breach, Defendant was aware of its security failures but failed to correct them or adequately and timely disclose them to the public, including Plaintiff and Class Members.

85. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendant knew or should have known that they did not make such actions and failed to implement adequate data security practices.

86. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PII and PHI of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' PII and PHI remains at risk of subsequent Data Breaches.

87. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Plaintiff and Class Members.

88. Defendant owed a duty to Plaintiff and Class Members to ensure that the Private Information it collected and was responsible for was adequately secured and protected.

89. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

90. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach that impacted the Private Information it collected and was responsible for in a timely manner.

91. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

92. Defendant owed a duty to Plaintiff and Class Members to disclose if its data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust this Private Information to Defendant.

93. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

94. Defendant owed a duty to Plaintiff and Class Members to mitigate the harm suffered by the Representative Plaintiff's and Class Members' as a result of the Data Breach.

95. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system and safeguards to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data, including identifying internal and external risks of a security breach;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits;

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

g. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information;

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons; and,

k. Retaining information past a recognized purpose and not deleting it.

The Federal Trade Commission Defines Defendant's Conduct as Constituting Unfair or Deceptive Acts

96. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See e.g., FTC v. Wyndham Corp.*, 799 F.3d 236 (3d Cir. 2015).

97. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[15]

[15] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf, (last visited January 31, 2024).

98. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, encrypt information stored on networks, understand its network's vulnerabilities, and implement policies to correct any security problems.[16]

99. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

100. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice.

101. Defendant was at all times fully aware of its obligations to protect Plaintiff's and Class Members' Private Information because of its business model of collecting and storing Private Information. Defendant was also aware of the significant adverse repercussions befalling healthcare recipients that would result from its failure to do so.

Value of the Relevant Sensitive Information

102. Although they provide greater efficiency and cost savings for providers, electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's, treatment plans) that is valuable to cyber criminals seeking to access them. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PII and PHI and financial information are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

[16] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed January 31, 2024).

103. The high value of PII and PHI and financial information to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[18]

104. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[19] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[20] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03% of overall health data breaches, according to cybersecurity firm Tenable.[21]

105. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

106. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other

---

[17] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-darkweb-how-much-it-costs/ last accessed January 31, 2024.

[18] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ last visited January 31, 2024.

[19] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 last visited January 31, 2024.

[20] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ last visited January 31, 2024.

[21] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches last visited January 31, 2024.

information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

107. Identity thieves can use PII and PHI and financial information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

108. There may be a time lag between when harm occurs versus when it is discovered and between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

109. The harm to Plaintiff and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical- related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which

[22] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf (last accessed January 31, 2024).

is more than identity thefts involving banking and finance, the government and the military, or education.[23]

110. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[24]

111. If cyber criminals manage to access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiff and Class Members.

112. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[25] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[26]

113. Data breaches are preventable.[27] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate

---

[23] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ (last accessed January 31, 2024).

[24] *Id.*

[25] See Elinor Mills, Study: Medical Identity Theft is Costly for Victims, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed January 31, 2024).

[26] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, available at https://www.experian.com/blogs/ask-experian/healthcare-data-breachwhat-to-know-about-them-and-what-to-do-after-one/ (last accessed January 31, 2024).

[27] Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

security solutions."[28] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[29]

114. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[30]

115. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with industry, standards, safeguards and concomitant duties established by HIPAA regulations.

Loss of the Benefit of the Bargain

116. As a consequence of Defendant's inadequate data security systems and protection, Plaintiff and Class Members have been deprived of the benefit of their bargain which occurred when they agreed to pay health care that contracted with Defendant for the provision of healthcare services. Plaintiff and Class Members, reasonable consumers – understandably expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendant had not provided the necessary adequate data security in any event. Consequently, Plaintiff and Class Members received services that were of a lesser value than what they had reasonably expected from and bargained for with Defendant.

Ongoing Need for Expensive Credit and Identity Theft Monitoring

117. Unquestionably there will be a future cost of credit and identify theft monitoring that will be necessary for Plaintiff and Class Members' protection going forward as a consequence of the Data Breach and the sensitive Private Information that has been accessed. The probability

[28] *Id*. at 17.

[29] *Id*. at 28.

[30] *Id.*

is strong that the stolen information will be used by criminals to accomplish crimes based on identity theft, including opening bank accounts and victims' names to make purchases or launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims. These fraudulent incidents may not be detected for years and individuals may not even know that they have yet occurred.

118. Credit monitoring and identity theft monitoring is expensive. The cost can run approximately $200 a year per each Class Member. This cost is necessary and reasonable, for Plaintiff and Class Members are now forced to monitor and protect themselves from identity theft going forward, and need to do so for many years.

Defendant's Inadequate Response to the Breach

119. Time is of the essence when highly sensitive PII and PHI is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII and PHI of Plaintiff and Class Members is likely available, or may be available at any moment, on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII and PHI, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing millions of Medicare numbers, Social Security numbers, Dates of birth, and other critical PHI and/or PII.

120. Despite this understanding, Defendant did not provide adequate and timely written notice of the Data Breach to Plaintiff and Class Members and has provided only scant details.

121. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.8% of U.S.-based workers are compensated on an hourly basis, while the other 44.2% are salaried.[31]

[31] U.S. BUREAU OF LABOR STATISTICS, Characteristics of minimum wage workers, 2021, available at https://www.bls.gov/opub/reports/minimum-wage/2021/pdf/home.pdf, (last visited

122. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[32] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[33] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

123. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

CLASS ALLEGATIONS

124. Pursuant to Fed. R. Civ. P. 23.01, *et seq*., Plaintiff asserts common law claims, as more fully alleged hereinafter, on behalf of the following proposed Class, defined as follows:

> All individuals whose Private Information was accessed or otherwise acquired or compromised as a result of the Data Breach.

Members of the Class are referred to herein collectively as "Class Members" or "Class."

125. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

126. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time, but Defendant provides services relating to millions of consumers and has acknowledged

---

January 18, 2024); *see also*, Bureau of Labor Statistics, https://www.bls.gov/news.release/empsit.t19.htm, last visited January 31, 2024 (finding that on average, private-sector workers make $1,146.99 per 40-hour work week).

[32] See https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html last visited January 31, 2024.

[33] *Id.*

that the number of individuals affected by the Data Breach was approximately 4.5 million persons, indicating that joinder of all members of the Class is impracticable. Ultimately, members of the Class will be readily identified through Defendant's records.

127. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard Plaintiff's and the Class Members' PII and PHI;

b) Whether Defendant failed to protect Plaintiff's and the Class Members' PII and PHI, as promised;

c) Whether Defendant's computer systems and data security practices used to protect Plaintiff's and the Class Members' PII and PHI violated state and local laws, or Defendant's duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and the Class Members' PII and PHI properly and/or as promised;

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair practice statutes, state privacy statutes, and state medical privacy statutes, HIPAA, and/or regulations, imposing duties upon Defendant, applicable to Plaintiff and Class Members;

f) Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class Members' PII and PHI;

h) Whether Defendant entered into contracts with Plaintiff and the Class

Members that included contract terms requiring Defendant to protect the confidentiality of Plaintiff's PII and PHI and have reasonable security measures;

i) Whether Defendant's conduct described herein constitutes a breach of its contracts with Plaintiff and each of the Class Members;

j) Whether Defendant should retain any money paid by Plaintiff and each of the Class Members to protect their PII and PHI;

k) Whether Plaintiff and the Class Members are entitled to damages as a result of Defendant's wrongful conduct;

l) Whether Plaintiff and the Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class Members.

128. **Typicality**: Plaintiff's claims are typical of the claims of each of the Class Members. Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

129. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and has the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

130. **Separateness**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the

proposed Class. Furthermore, the Private Information collected by Defendant still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the PHI and PII collected, stored, and maintained by Defendant.

131. **Class-wide Applicability**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

132. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT I

Negligence
(On Behalf of Plaintiff and the Class)

133. Plaintiff, on behalf of himself and the Class, re-alleges and incorporates the above allegations by reference.

134. Plaintiff and Class Members were required to submit PII and PHI to healthcare providers, including Defendant, in order to obtain insurance coverage and/or to receive healthcare services.

135. Defendant knew, or should have known, of the risks and responsibilities inherent in collecting and storing the PII and PHI of Plaintiff and Class Members.

136. As described above, Defendant owed a duty of care to Plaintiff and Class Members whose PII and PHI had been entrusted to Defendant.

137. Defendant breached its duty to Plaintiff and Class Members by failing to secure their PII and PHI from unauthorized disclosure to third parties.

138. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' PII and PHI.

139. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members because it collected and/or stored the PII and PHI of Plaintiff and the Class Members.

140. But for Defendant's wrongful and negligent breach of their duty owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

141. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duty. Defendant knew or should have known it was failing to meet its duty, and that Defendant's breach of its duty would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized exposure of their PII and PHI.

142. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II

Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

143. Plaintiff, on behalf of himself and the Class, re-alleges and incorporates the above allegations by reference.

144. Defendant had a legal duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI.

145. Defendant breached its duty to Plaintiff and Class Members by failing to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI from unauthorized access.

146. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

147. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

148. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duty. Defendant knew or should have known that it was failing to meet its duty, and that Defendant's breach of that duty would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized access to their PII and PHI.

149. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class)

150. Plaintiff, on behalf of himself and the Class, re-alleges and incorporates the above allegations by reference.

151. Plaintiff and Class Members entered into valid, binding, and enforceable express or implied contracts with entities affiliated with or serviced by Defendant, as alleged above.

152. The contracts respecting which Plaintiff and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform its contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendant would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiff's PII and PHI from unauthorized disclosure and to comply with state laws and regulations.

153. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members who sought medical services from Defendant and, in doing so, entrusted Defendant, pursuant to its requirements and its HIPPA Notice, with their PII and PHI.

154. Despite this special relationship with Plaintiff, Defendant did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' PII and PHI.

155. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant.

156. Defendant's failure to act in good faith in complying with the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received healthcare and related services that were less valuable than what they paid for and less valuable than their reasonable expectations.

157. Accordingly, Plaintiff and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing respecting which they are express or implied beneficiaries, and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV

Breach of Duty
(On Behalf of Plaintiff and the Class)

158. Plaintiff, on behalf of himself and the Class, re-alleges and incorporates the above allegations by reference.

159. Defendant accepted the special confidence placed in them as a HIPAA Business Associate, understanding that it would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of the PII and PHI of Plaintiff and Class Members.

160. Defendant became the guardian of Plaintiff's and Class Members' PII and PHI and accepted a fiduciary duty to safeguard Plaintiff's and the Class Members' PII and PHI.

161. Defendant's fiduciary duty to act for the benefit of Plaintiff and Class Members pertains as well to matters within the scope of Defendant's relationship with its clients, in particular, to keep secure the PII and PHI of Plaintiff and Class Members.

162. Defendant breached its fiduciary duty to Plaintiff and Class Members by (a) failing to protect their PII and PHI; (b) by failing to notify Plaintiff and the Class Members of the unauthorized disclosure of the PII and PHI; and (c) by otherwise failing to safeguard Plaintiff's and the Class Members' PII and PHI.

163. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and/or Class Members have suffered and/or will suffer injury, including but not limited to: (a) the compromise of their PII and PHI; and (b) the diminished value of the services they received as a result of unauthorized exposure of Plaintiff's and Class Members' PII and PHI.

164. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V

Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

165. Plaintiff, on behalf of himself and the Class, re-alleges and incorporates the above allegations by reference.

166. Defendant collected and maintained responsibility for the Private Information of Plaintiff and the Class, including, *inter alia*, name, Social Security Number, and other PHI in connection with the provision of services to Plaintiff and the Class.

167. At the time Defendant acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

168. The PHI and PII of Plaintiff and the Class would not have entrusted to Defendant had it been known known that Defendant would fail to adequately safeguard said PHI and PII.

169. Implicit in the agreement between healthcare providers and Defendant was Defendant's obligation to: (a) use PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

170. Plaintiff and the Class are third party beneficiaries of the contracts, implied or otherwise, between health care providers and Defendant.

171. In collecting and maintaining responsibility for the maintenance and protection of the PII of Plaintiff and the Class and publishing the HIPAA Policy, Defendant entered into contracts with Plaintiff and the Class requiring Defendant to protect and keep secure the PHI/PII of Plaintiff and the Class.

172. Defendant breached the contracts it made with health care providers by failing to protect and keep secure the PHI/PII of Plaintiff and the Class.

173. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and/or impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

174. As a direct and proximate result of Defendant's breach of contract, Plaintiff and the Class are at an increased risk of identity theft or fraud.

175. As a direct and proximate result of Defendant's breach of contract, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, prays for relief and judgment against Defendant as follows:

A. certifying the Class as defined herein, appointing Plaintiff as representative of the Class, and designating Plaintiff's counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiff and the Class on all counts asserted herein;

D. awarding Plaintiff and the Class compensatory damages and actual damages in an amount to be determined by proof;

E. awarding Plaintiff and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiff and the Class punitive damages;

G. awarding Plaintiff and the Class civil penalties;

H. granting Plaintiff and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

I. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: February 2, 2024

Respectfully submitted,

BARRACK, RODOS & BACINE

/s/ *Andrew J. Heo*
Andrew J. Heo (N.J. Bar No. 296062019)
One Gateway Center, Suite 2600
Newark, NJ 07102
Tel: (973) 297-1484
Fax: (973) 297-1485
aheo@barrack.com

BARRACK, RODOS & BACINE

Samuel M. Ward*
600 W Broadway #900
San Diego, CA 92101
Tel: (619) 230-0800
Fax: (619) 230-1874
sward@barrack.com

EMERSON FIRM, PLLC

John G. Emerson*
2500 Wilcrest Drive, Suite 300
Houston, TX 77042
Tel: (800) 551-8649
Fax: (501) 286-4659
jemerson@emersonfirm.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice applications forthcoming*